

**REMARKS****Status of case**

Claims 1 through 24 are currently pending in this case.

**Rejection under 35 U.S.C. § 112**

Claim 1 was rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In particular, the Office Action stated that the limitation “said restriction information” lacks antecedent basis. Applicants amend the claim where it is believed appropriate to overcome the rejection.

**Rejection under 35 U.S.C. § 103**

Claims 1, 3 and 4 were rejected under 35 U.S.C. §103(a) as being unpatentable over Traw et al. (U.S. Patent No. 5,949877) in view of Risan et al. (U.S. Patent Application No. 2003/0221127). Claim 2 was considered allowable if rewritten in independent format.

The Traw reference discloses a device having the function of securely transferring content to another device. In particular, the Traw reference focuses on problems during the transfer of the content from one device to another. For example, the summary of the invention in the Traw reference states the following:

**Briefly, a method for protecting digital content from copying and/or other misuse as it is transferred between devices over insecure links, includes authenticating that both a content source and a content sink are compliant devices, establishing a secure control channel between the content source and the content sink, establishing a secure content channel, providing content keys, and transferring content.**

Col. 1, lines 42-48 (emphasis added); *see also* col. 2, lines 51-60.

The Risan reference teaches a system that includes multiple client devices, with the client devices in their respective vicinity of the world. Paragraph [0011]. The Risan reference further teaches that once a client device receives media, “it is stored using hidden directories to prevent easy redistribution with other devices. An access key procedure and rate control restrictor may

also be implemented to monitor and restrict suspicious media requests.” Paragraph [0011]. The Risan reference teaches that the access key procedure requires having “a time sensitive access key (e.g., for that day, hour, or for any defined timeframe) thereby enabling the client 204 to eventually receive the requested media content.” Paragraph [0051]. The Risan reference further teaches that the rate control restrictor functions as follows:

a rate control restrictor functionality may be resident to content server 212 in order to monitor and limit “suspicious” media content retrieval. For instance, if a client device (e.g., 204) tries to retrieve media content from content server 212 faster than a predefined limit, the rate control restrictor uncouples client device 204 from its media content source (e.g., content server 212) and continues to restrict its access from the source for a predefined amount of time, as described herein.

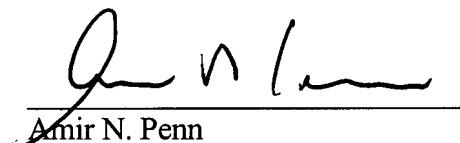
Paragraph [0058]. Thus, the Risan reference teaches that these types of features, including the access key procedure and rate control restrictor, restrict redistribution of delivered media content. Paragraph [0011].

In contrast to the cited references, one aspect of the invention includes determining whether to transmit content based on whether the device receiving the content has the functionality of restricting distribution of the content, *i.e.*, “whereby the another communication device prevents transmitting the content, which was transmitted from the communication device, to a third communication device based on said redistribution restriction information.” See claims 1 and 4. Unlike the Traw and Risan references, the claims as presented examine what the device receiving the content will do with the content after receipt of the content, specifically will the device that receives the content restrict redistribution of the content. This is different from the cited references, which do not examine what will be done with the content after receipt. For example, the Traw reference focuses on security of the content during transmission from one device to another. As another example, the Risan reference focuses on whether the requesting device is currently authorized to request the content. Specifically, the Risan reference uses access keys and rate control restrictors to determine whether the request itself is acceptable. This is significantly different from the present invention, as claimed, which examines what the receiving device will do with the content (*e.g.*, restrict distribution) after receipt of the content. Therefore, the claims as currently presented are patentable over the cited references.

**SUMMARY**

Applicant respectfully requests the Examiner to grant early allowance of this application. The Examiner is invited to contact the undersigned attorneys for the Applicant via telephone if such communication would expedite this application.

Respectfully submitted,



Amir N. Penn  
Registration No. 40,767  
Attorney for Applicant

BRINKS HOFER GILSON & LIONE  
P.O. BOX 10395  
CHICAGO, ILLINOIS 60610  
(312) 321-4200